PODER JUDICIÁRIO
TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO
SEÇÃO DE ANÁLISE E LICITAÇÃO

Pregão Eletrônico nº 52/2019

OBJETO: Aquisição de solução de firewall composta de duas appliances em alta disponibilidade (HA) ativo/ativo.

Aplicação do Decreto 7174/2010, como critério de desempate

(Processo Produtivo Básico e/ou Tecnologia Desenvolvida no País)

Ampla Concorrência

São Luís
- 2019 –

TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO
SEÇÃO DE ANÁLISE E LICITAÇÃO

EDITAL
PREGÃO ELETRÔNICO nº 52/2019
PROCESSO ADMINISTRATIVO DIGITAL Nº 10.973/2019

PREÂMBULO

O Tribunal Regional Eleitoral do Maranhão-TRE, neste ato designado **TRIBUNAL** torna público para conhecimento de todos que fará realizar, às **14:00 horas (horário de Brasília), do dia 22/11/2019,** sob o comando do Pregoeiro Oficial, designado pela **PORTARIA Nº 1195/2017**, de 28 de dezembro de 2017, do Presidente do **TRE-MA,** por meio do uso de tecnologia da informação, Licitação na modalidade **PREGÃO,** na **FORMA ELETRÔNICA,** do tipo **MENOR PREÇO**, mediante as condições estabelecidas neste Edital e seus anexos, decorrentes do Processo Administrativo Digital nº **10.973/2019**.

A Licitação será regida pela **LEI Nº 10.520/2002**, **LEI COMPLEMENTAR Nº 123/2006, LEI COMPLEMENTAR Nº 147/2014,** subsidiariamente a **LEI Nº 8.666/1993, DECRETO Nº 5.450/2005, DECRETO Nº 8.538/2015, DECRETO N° 7.174/2010** e demais normas aplicáveis à matéria, naquilo que não contrarie este edital e pelas cláusulas e condições abaixo declinadas.

A Sessão Pública será realizada através do site www.comprasgovernamentais.gov.br e conduzida pelo **PREGOEIRO**, na sala da **COMISSÃO PERMANENTE DE LICITAÇÃO**, no 1º andar do Anexo ao prédio sede do **TRIBUNAL**, na Avenida Senador Vitorino Freire, s/nº - Bairro Areinha, nesta cidade de São Luís, Estado do Maranhão.

Todos os horários estabelecidos neste edital, no aviso e durante a Sessão Pública observarão, para todos os efeitos, o horário de Brasília, Distrito Federal, inclusive para contagem de tempo e registro no **SISTEMA ELETRÔNICO**, daqui por diante denominado **SISTEMA**, e na documentação relativa ao certame.

Ocorrendo decretação de feriado ou outro fato superveniente que impeça a realização desta Licitação na data acima mencionada, o evento será automaticamente transferido para o primeiro dia útil subseqüente, independentemente de nova comunicação.

1. DO OBJETO

1.1. Constitui objeto do presente **PREGÃO a aquisição de solução de firewall, conforme especificações deste edital e seus anexos e abaixo:**

Grupo	Item	Descrição	Unidade	Quantidade
1	1	Solução de firewall (equipamento principal + equipamento de alta garantia) com instalação assistida, configuração e com garantia de 60 meses	UN	2
	2	Solução de firewall de pequeno porte, com instalação assistida, configuração e com garantia de 60 meses	UN	20

1.2. A prestação de serviços objeto desta Licitação deverá ser realizada em rigorosa observância ao Termo de Referência – Anexo I deste Edital e as normas vigentes que a ele se aplicarem.

1.3. O custo total máximo para o objeto desta Licitação foi estimado pelo **TRIBUNAL** em **R$ 1.023.605,05 (um milhão, vinte e três mil seiscentos e cinco reais e cinco centavos),** conforme detalhamento no Termo de Referência – Anexo I deste Edital.

1.4. Em caso de discordância existente entre as especificações dos objetos descritas no **SISTEMA** e as especificações técnicas constantes do Edital, prevalecerão as do Edital.

2. DAS CONDIÇÕES PARA PARTICIPAÇÃO

2.1. Poderão participar deste **PREGÃO** as empresas que atenderem a todas as exigências deste Edital, inclusive quanto à documentação constante neste edital e em seus anexos.

2.2. A Secretaria de Logística e Tecnologia da Informação – SLTI, do Ministério do Planejamento, Orçamento e Gestão, atuará como provedor do **SISTEMA ELETRÔNICO COMPRASGOVERNAMENTAIS**, daqui por diante denominado **SISTEMA**.

2.3. O **TRIBUNAL** não se responsabilizará por eventual desconexão sua ou dos LICITANTES ao referido **SISTEMA**.

2.4. Não poderão participar deste **PREGÃO**:

a) Empresa que se encontre em regime de recuperação judicial ou extrajudicial ou ainda com pedido de falência, concurso de credores, processo de insolvência (salvo se o respectivo plano de recuperação foi acolhido judicialmente, na forma do art. 58, da Lei n.º 11.101, de 09 de fevereiro de 2005);

b) Empresa estrangeira não autorizada a funcionar no país.

c) Empresa que tenha sido declarada inidônea para licitar ou contratar com a Administração Pública, Direta ou Indireta, Federal, Estadual ou Municipal ou do Distrito Federal, enquanto perdurarem os motivos da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade.

d) Empresa impedida de licitar e contratar com a União ou suspensa temporariamente de licitar e impedida de contratar com este Tribunal.

e) Empresa cujo objeto social não seja pertinente e compatível com o objeto deste **PREGÃO**.

f) Empresa que tenha em seu quadro societário cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau, inclusive, dos magistrados ocupantes de cargos de direção ou no exercício de funções administrativas, assim como de servidores ocupantes de cargos de direção, chefia e assessoramento.

g) Empresa cujos proprietários e ou/ sócios exerçam mandato eletivo capaz de ensejar os impedimentos previstos no art. 29, inciso IX c/c e art. 54, I, "a" e II, "a", da Constituição Federal.

2.5. O LICITANTE deverá manifestar, através de **Declaração Específica**, disponibilizada pelo **SISTEMA**, o pleno conhecimento e atendimento às exigências de habilitação para o presente **PREGÃO**, bem como que a PROPOSTA está em conformidade com as exigências editalícias, sujeitando-se às sanções previstas neste instrumento convocatório, na hipótese de declaração falsa.

2.6. Nos itens (ou grupos, se for o caso) com preço total de referência igual ou inferior a R$ 80.000,00 (oitenta mil reais), expressamente indicados no Termo de Referência - Anexo I deste edital, somente poderão participar empresas que atenderem a todas as exigências deste Edital e estiverem, nos termos do artigo 3º, incisos I e II, da Lei Complementar nº 123, de 14 de dezembro de 2006, enquadradas como **Microempresas** ou **Empresas de Pequeno Porte** e,

ainda, devidamente credenciadas na Secretaria de Logística e Tecnologia da Informação – SLTI, do Ministério do Planejamento, Orçamento e Gestão, através do site www.comprasgovernamentais.gov.br.

2.7. Para efeitos de participação das **Microempresas** ou **Empresas de Pequeno Porte** nesta licitação, nos termos do art. 3º, inciso I, da Lei Complementar nº 123/2006, são considerados:

a) **Microempresa** – o empresário, a pessoa jurídica, ou a ela equiparada, que aufira, em cada ano-calendário, receita bruta igual ou inferior a R$ 360.000,00 (trezentos e sessenta mil reais).

b) **Empresa de Pequeno Porte** – o empresário, a pessoa jurídica, ou a ela equiparada, que aufira, em cada ano-calendário, receita bruta superior a R$ 360.000,00 (trezentos e sessenta mil reais) e igual ou inferior a R$ 4.800.000,00 (quatro milhões e oitocentos mil reais).

2.8. Não fará jus ao regime diferenciado e favorecido nas licitações públicas previsto na Lei Complementar nº 123/2006 a Microempresa ou Empresa de Pequeno Porte:

a) de cujo capital participe outra pessoa jurídica;

b) que seja filial, sucursal, agência ou representação, no País, de pessoa jurídica com sede no exterior;

c) de cujo capital participe pessoa física que seja inscrita como empresário ou seja sócia de outra empresa que receba tratamento jurídico diferenciado, nos termos da referida Lei Complementar, desde que a receita bruta global ultrapasse o limite de que trata o art. 3º, inciso II, da Lei Complementar Nº 123/2006;

d) cujo titular ou sócio participe com mais de 10% (dez por cento) do capital de outra empresa não beneficiada por esta Lei Complementar, desde que a receita bruta global ultrapasse o limite de que trata o art. 3º, inciso II, da Lei Complementar Nº 123, de 14 de dezembro de 2006;

e) cujo sócio ou titular seja administrador ou equiparado de outra pessoa jurídica com fins lucrativos, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do caput do art. 3º da Lei Complementar Nº 123, de 14 de dezembro de 2006;

f) constituída sob a forma de cooperativa, salvo as de consumo;

g) que participe do capital de outra pessoa jurídica;

h) que exerça atividade de banco comercial, de investimentos e de desenvolvimento, de caixa econômica, de sociedade de crédito, financiamento e investimento ou de crédito imobiliário, de corretora ou de distribuidora de títulos, valores mobiliários e câmbio, de empresa de arrendamento mercantil, de seguros privados e de capitalização ou de previdência complementar;

i) resultante ou remanescente de cisão ou qualquer outra forma de desmembramento de pessoa jurídica que tenha ocorrido em um dos 5 (cinco) anos-calendário anteriores;

j) constituída sob a forma de sociedade por ações.

2.9. As Microempresas e Empresas de Pequeno Porte participantes desta licitação deverão comprovar seu enquadramento e condição através de Declaração Especifica registrada em campo específico do **SISTEMA,** nos termos do **subitem 5.4** deste Edital, facultado ao **TRIBUNAL** se for o caso, promover diligência com a finalidade de comprovar o enquadramento do licitante como Microempresa ou Empresa de Pequeno Porte diante das normas da Lei.

2.10. O enquadramento, reenquadramento e desenquandramento das Microempresas e Empresas de Pequeno Porte, consoante dispõe o artigo 3º e seus parágrafos, da Lei Complementar nº. 123/2006 será comprovado através de Certidões Específicas emitidas pelas Juntas Comerciais, nos termos do art. 1º da Instrução Normativa nº 10, de 05 de dezembro de 2013, do Departamento de Registro Empresarial e Integração - DREI.

2.11. O licitante responsabilizar-se-á por todas as transações que forem efetuadas em seu nome no **SISTEMA**, assumindo como firmes e verdadeiras suas propostas, assim como os lances inseridos durante a sessão pública.

2.12. Na hipótese de haver diferença na descrição do objeto registrada no **SISTEMA** (www.comprasgovernamentais.gov.br) e nas especificações constantes no Termo de Referência - **ANEXO I** deste Edital, deverá ser considerada a do Edital.

3. DA REPRESENTAÇÃO E DO CREDENCIAMENTO

3.1. A empresa interessada em participar deste **PREGÃO** deverá providenciar, previamente, o credenciamento perante a Secretaria de Logística e Tecnologia da Informação, do Ministério do Planejamento, Orçamento e Gestão, provedor do **SISTEMA** utilizado nesta Licitação, no site www.comprasgovernamentais.gov.br, devendo também cadastrar-se no Sistema de Cadastramento Unificado de Fornecedores – SICAF.

3.2. O credenciamento do interessado dar-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao **SISTEMA**.

3.3. O credenciamento do LICITANTE, bem como a sua manutenção, dependerá de registro Cadastral atualizado no Sistema de Cadastramento Unificado de Fornecedores – SICAF.

3.4. O credenciamento junto ao provedor do **SISTEMA** implica responsabilidade legal do LICITANTE ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes ao **PREGÃO**, assumindo como firmes e verdadeiras suas PROPOSTAS e lances, inclusive os atos por eles praticados.

3.5. O LICITANTE credenciado deve acompanhar as operações do **SISTEMA** durante o procedimento licitatório, responsabilizando-se pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo **SISTEMA** ou de sua desconexão.

3.6. O uso da senha de acesso ao **SISTEMA** pelo LICITANTE é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do **SISTEMA** ou ao **TRIBUNAL** responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que provocados por terceiros.

4. DAS DATAS DO RECEBIMENTO E DA ABERTURA DAS PROPOSTAS

4.1. Os LICITANTES deverão observar as datas e horários, com base no horário de Brasília, previstos para a realização deste **PREGÃO**, nos termos que seguem:

a) Data de recebimento das **Propostas**	Do dia 06/11/2019 até as 14:00 horas do dia 22/11/2019
b) Data da abertura das **Propostas**	Às 14:00 horas do dia 22/11/2019

5. DA PROPOSTA DE PREÇOS

5.1 A PROPOSTA DE PREÇOS deverá ser formulada de acordo com as especificações constantes do ANEXO I deste Edital e registrada no **SISTEMA**, sendo obrigatório o preenchimento do campo **descrição complementar**, onde deverão ser transcritas as especificações dos serviços a serem prestados de forma clara e precisa.

5.2 Até a data e hora de início da Sessão Pública prevista neste Edital, o LICITANTE poderá acessar o **SISTEMA** para retirar, alterar ou complementar a PROPOSTA DE PREÇOS formulada. Após o início da Sessão a PROPOSTA DE PREÇOS não poderá mais sofrer alterações ou ser retirada.

5.3 As PROPOSTAS DE PREÇOS dos concorrentes deste **PREGÃO** contendo a descrição dos serviços, os valores e demais especificações exigidas e eventuais anexos ficarão disponíveis na *internet*.

5.4 O LICITANTE, no ato de envio de sua proposta, deverá encaminhar, de forma virtual, utilizando a funcionalidade existente no sistema de pregão eletrônico, as seguintes declarações:

a) Inexistência de fato superveniente que o impeça de participar do certame;

b) Cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal;

c) Concordância com as condições estabelecidas neste Edital e que atende aos requisitos de HABILITAÇÃO;

d) Atendimento aos requisitos do art. 3º da Lei Complementar nº 123/2006, para microempresas e empresas de pequeno porte, se for o caso;

e) Elaboração independente de proposta, consoante Instrução Normativa nº 02, de 17 de setembro de 2009 do Ministério, Orçamento e Gestão.

5.5 A falsidade das DECLARAÇÕES prestadas pelo LICITANTE caracteriza crime previsto no artigo 299 do Código Penal, sujeitando-o ainda às sanções previstas no **Decreto nº 5.450/2005**.

5.6 Os itens da PROPOSTA DE PREÇOS que eventualmente contemplem objetos que não correspondam às especificações contidas no ANEXO I deste Edital serão desconsiderados.

5.7 Se o LICITANTE declarar, em campo próprio do SISTEMA, que atende aos requisitos do art. 3º da LEI COMPLEMENTAR Nº 123/2006 para fazer *jus* aos benefícios previstos nesta Lei, fica facultado ao TRIBUNAL promover diligência com a finalidade de comprovar o seu enquadramento.

6. DA ABERTURA DA SESSÃO PÚBLICA

6.1 O **PREGOEIRO**, via **SISTEMA**, dará início ao **PREGÃO** com a abertura da Sessão Pública, na data e horário indicados no preâmbulo deste edital, com a divulgação das PROPOSTAS DE PREÇOS recebidas em conformidade com as normas conduzidas no **ITEM 5** deste Edital.

6.2 A comunicação entre o **PREGOEIRO** e os LICITANTES ocorrerá exclusivamente mediante troca de mensagem, em campo próprio do **SISTEMA**.

6.3 Cabe ao LICITANTE acompanhar as operações no **SISTEMA** durante a **Sessão Pública** do **PREGÃO**, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem emitida pelo **SISTEMA** ou de sua desconexão.

6.4 O **SISTEMA** ordenará, automaticamente, as PROPOSTAS classificadas pelo **PREGOEIRO**, sendo que somente estas participarão da fase de lances.

6.5 Ordenadas as **PROPOSTAS**, o **PREGOEIRO** dará início à fase competitiva, quando então os LICITANTES poderão encaminhar lances sucessivos, exclusivamente por meio do **SISTEMA**.

6.6 Da Sessão Pública do **PREGÃO** será lavrada ata circunstanciada e imediatamente disponibilizada na *internet* pelo **SISTEMA**, para acesso livre.

7. DA FASE COMPETITIVA COM A FORMULAÇÃO DE LANCES

7.1 Aberta a etapa competitiva, os licitantes poderão encaminhar seus lances**,** observando o horário fixado e as regras de aceitação dos mesmos. A cada lance ofertado, o licitante será imediatamente informado do seu recebimento e do valor consignado no registro.

7.2 Os lances serão ofertados pelo **VALOR TOTAL DO ITEM**, nas condições definidas no Termo de Referência - **ANEXO I** deste edital;

7.3 O licitante somente poderá oferecer lance inferior ao último por ele ofertado e registrado pelo **SISTEMA.**

7.4 Não serão aceitos dois ou mais lances iguais, prevalecendo aquele que for recebido e registrado primeiro.

7.5 Durante a Sessão Pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante detentor do lance.

7.6 A etapa de lances da Sessão Pública será colocado em aviso de iminência para encerramento por decisão do **PREGOEIRO**. O **SISTEMA** encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá período de tempo de até 30 (trinta) minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

7.7 Não poderá haver desistência dos lances efetuados, sujeitando-se a proponente desistente às penalidades previstas no art. 28 do Decreto n. 5.450/05.

7.8 Durante a fase de lances o **PREGOEIRO** poderá excluir, justificadamente, lance cujo valor seja considerado inexeqüível, desclassificando a proposta do licitante.

7.9 Após o encerramento da etapa competitiva de lances, o **PREGOEIRO** poderá encaminhar, pelo **SISTEMA,** contraproposta ao licitante que tenha apresentado lance mais vantajoso, para que seja obtida melhor proposta, observado o critério de julgamento, não se admitindo negociar condições diferentes daquelas previstas no edital. A negociação poderá ser acompanhada pelos demais licitantes.

7.10 No caso de desconexão do **PREGOEIRO** no decorrer da etapa de lances**,** se o **SISTEMA** permanecer acessível aos licitantes os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

7.11 Quando a desconexão do **PREGOEIRO** persistir por tempo superior a 10 (dez) minutos, a Sessão do **PREGÃO** poderá será suspensa e reiniciada após a comunicação expressa aos licitantes, no endereço eletrônico utilizado para divulgação.

7.12 Nos itens (ou grupos, se for o caso) com preço total de referência superior a R$ 80.000,00 (oitenta mil reais), expressamente indicados no Termo de Referência - Anexo I deste Edital, encerrada a etapa de lances será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial, devendo, ainda, a própria empresa declarar, em campo próprio do **SISTEMA**, que atende aos requisitos do art. 3º da LEI COMPLEMENTAR Nº 123/2006 para fazer jus aos benefícios previstos ali previstos.

7.12.1 O sistema identificará em coluna própria as licitantes qualificadas como microempresas ou empresas de pequeno porte, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentado pelo Decreto nº 8.538, de 2015.

7.12.2 Caso a melhor oferta válida tenha sido apresentada por empresa de maior porte, as propostas de licitantes qualificadas como microempresas ou empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da proposta ou lance de menor preço serão consideradas empatadas com a primeira colocada.

7.12.3 A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

7.12.4 Caso a licitante qualificada como microempresa ou empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes qualificadas como microempresa ou empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

7.12.5 Sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

7.13 Após o encerramento da fase de lances e do desempate de que trata o item anterior, o Pregoeiro concederá o prazo de 2 (duas) horas para que os licitantes comuniquem, exclusivamente por meio eletrônico, através do endereço licitacao@tre-ma.jus.br que fazem jus ao uso do direito de preferência do Decreto n. 7174/2010, juntando a documentação de que tratam os itens 8.9 e 8.10.

7.13.1 A falta de comunicação na forma e prazo anterior importará na decadência ao direito de preferência do Decreto n. 7174/2010.

8. DA PROPOSTA ESCRITA DE PREÇOS

8.1. Finda a fase de lances, o licitante detentor do **MENOR LANCE** deverá encaminhar no prazo máximo de **20 (vinte) horas**, por meio eletrônico, sua **PROPOSTA ESCRITA DE PREÇOS** com o valor readequado ao valor do lance vencedor, bem como os demais dados constantes do **subitem 8.3** deste edital, para sua elaboração.

8.2. O não envio da **PROPOSTA ESCRITA DE PREÇOS** pelo LICITANTE no prazo estabelecido implicará desclassificação do LICITANTE, decadência do direito à contratação, sem prejuízo de multa, limitada a 30% (trinta por cento) do valor da contratação, impedimento de licitar e contratar com a União, pelo prazo de até 5 (cinco) anos, e descredenciamento no SICAF, cabendo ao PREGOEIRO convocar os LICITANTES na ordem remanescente dos lances e dar continuidade ao PREGÃO.

8.3. A **PROPOSTA ESCRITA DE PREÇOS** deverá conter as seguintes informações:

a) Razão Social da Empresa, com endereço e numero do CNPJ/MF;

b) Preços unitários e totais dos ITENS e do GRUPO, consoante tabela de formação de preços constante do Termo de Referência **ANEXO I** do Edital e abaixo, em reais, em algarismos, inclusos todas as despesas que resultem no custo das aquisições, tais como impostos, taxas, transportes, materiais utilizados, seguros, encargos fiscais e todos os ônus diretos e quaisquer outras despesas, que incidirem na execução dos serviços.

Grupo	Item	Descrição	Unidade	Quantidade	Valor Unitário	Valor Total
1	1	Solução de firewall (equipamento principal + equipamento de alta garantia) com instalação assistida, configuração e com garantia de 60 meses	UN	2	R$ ..... (.....)	R$ ..... (.....)
	2	Solução de firewall de pequeno porte, com instalação assistida, configuração e com garantia de 60 meses	UN	20	R$ ..... (.....)	R$ ..... (.....)
Valor total do Grupo 1:					R$ ..... (.....)	

b.1) Os preços propostos não poderão ser superiores aos valores estabelecidos no Termo de Referência, sob pena de desclassificação da proposta;

c) Prazo de validade**,** que não poderá ser inferior a 60 (sessenta) dias a contar da data da Sessão Pública designada no preâmbulo deste edital;

d) Características dos serviços/produtos ofertados, de acordo com as especificações constantes do Termo de Referência - **ANEXO I** deste edital.

e) Dados da empresa licitante tais como: telefone, e-mail, banco, agência, número da conta-corrente e praça de pagamento (facultada a apresentação destas informações quando da contratação);

f) Declaração de que o serviço/produto ofertado foi produzido com tecnologia desenvolvida no país e/ou de acordo com o Processo Produtivo Básico (PPB), para fazer uso do direito de preferência do Decreto n. 7174/2010, se for o caso.

8.3.1 A Licitante vencedora estará obrigada a comprovar, em se tratando de bens ou serviços de informática ou automação, a origem dos bens importados oferecidos e a quitação dos tributos de importação a eles referentes, que deve ser apresentada no momento da entrega do objeto, sob pena de rescisão contratual e multa de 10% (dez por cento) sobre o valor do contrato/empenho.

8.4. Uma vez aberta a **PROPOSTA ESCRITA DE PREÇOS,** não serão admitidas retificações de preços ou alterações nas condições estipuladas, nem tampouco com mais de uma cotação, exceto no caso de disputa por meio de lances inseridos no **SISTEMA**, conforme previsto neste edital.

8.5. Decorrido o prazo de validade da **PROPOSTA ESCRITA DE PREÇOS** sem convocação para a contratação, ficam os licitantes liberados dos compromissos assumidos, cabendo, no caso, negociação com o **TRIBUNAL** para manter o preço proposto.

8.6. O **TRIBUNAL** poderá solicitar ao licitante a prorrogação do prazo de validade da **PROPOSTA ESCRITA DE PREÇOS** por até 30 (trinta) dias. Neste caso, tanto a solicitação quanto a aceitação serão formuladas por escrito, sendo facultado ao licitante recusar ou aceitar o pedido; entretanto, no caso de concordância, a **PROPOSTA ESCRITA DE PREÇOS** não poderá ser modificada.

8.7. Verificando-se discordância entre o preço unitário e o total da **PROPOSTA ESCRITA DE PREÇOS,** prevalecerá o primeiro, sendo corrigido o preço total; ocorrendo divergência entre valores numéricos e os por extenso, prevalecerão os últimos. Se o licitante não aceitar a correção de tais erros, sua **PROPOSTA ESCRITA DE PREÇOS** será rejeitada, convocando-se a empresa subseqüentemente classificada, se houver.

8.8. Todos os custos decorrentes da elaboração e apresentação da **PROPOSTA ESCRITA DE PREÇOS** serão de responsabilidade exclusiva do licitante.

8.9. **Caso a licitante queira fazer uso dos benefícios previstos no art. 6º do Decreto nº. 7174/2010, deverá comprovar o atendimento ao Processo Produtivo Básico, mediante a apresentação do documento comprobatório à fruição dos incentivos fiscais regulamentados pelo Decreto n. 5.906, de 26 de setembro de 2006, ou pelo Decreto n. 6.008, de 29 de dezembro de 2006, emitido pela Superintendência da Zona Franca de Manaus ou pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações.**

8.10. **Caso a licitante queira fazer uso dos benefícios previstos no art. 6º do Decreto nº. 7174/2010, deverá comprovar o atendimento à condição de bens ou produtos com tecnologia desenvolvida no País, mediante a apresentação do documento comprobatório à fruição dos incentivos fiscais regulamentados pela Portaria MCT nº 950, de 12 de dezembro de 2006, emitido pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações.**

9. DO JULGAMENTO E ACEITABILIDADE DA PROPOSTA

9.1. O **PREGOEIRO** examinará a PROPOSTA classificada em primeiro lugar quanto à compatibilidade do preço em relação ao determinado para a contratação e as especificações constantes do Termo de Referência - ANEXO I e verificará, em seguida, a habilitação do LICITANTE nas condições definidas no **ITEM 10** deste edital. Serão observadas no julgamento das PROPOSTAS as seguintes condições:

9.1.1. No julgamento das PROPOSTAS, a classificação dar-se-á pelo critério de MENOR PREÇO, sendo considerada vencedora a PROPOSTA que atender às condições do Edital e ofertar o MENOR LANCE.

9.1.2. O critério de aceitabilidade do melhor preço terá como parâmetro o valor máximo determinado pelo EDITAL.

9.1.3. Serão desclassificadas as PROPOSTAS que não atenderem às condições exigidas no Edital, apresentarem preços acima do máximo estabelecido ou forem manifestamente inexequíveis.

9.1.4. As PROPOSTAS com preços inexequíveis são consideradas aquelas cujo LICITANTE não venha a demonstrar, mediante solicitação do **PREGOEIRO**, sua viabilidade através de documentação que comprove que os custos dos insumos são coerentes com os de mercado e que os coeficientes de produtividade são compatíveis com a execução do objeto do contrato.

9.1.5. O **PREGOEIRO**, no julgamento das PROPOSTAS, poderá realizar diligências ou requisitar informações, incluindo esclarecimentos e detalhamentos sobre as PROPOSTAS, sem implicar modificação de seu teor ou inclusão de documento ou informação que deveria constar originalmente na PROPOSTA. A não apresentação das informações solicitadas implicará o julgamento no estado em que se encontram as PROPOSTAS, podendo resultar em sua desclassificação.

9.2. O **PREGOEIRO** poderá solicitar também pareceres de técnicos para orientar sua decisão.

9.3. Se a PROPOSTA não for aceitável ou se o LICITANTE não atender às exigências editalícias, o **PREGOEIRO** examinará as PROPOSTAS subsequentes, na ordem de classificação, até a apuração de uma PROPOSTA que atenda a todas as exigências do Edital. O **PREGOEIRO** poderá negociar com o Proponente para que seja obtido preço melhor.

9.4. No julgamento das PROPOSTAS, o **PREGOEIRO** poderá sanar erros ou falhas que não alterem a substância da PROPOSTA, mediante despacho fundamentado, registrado em Ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de classificação.

10. DA HABILITAÇÃO

10.1. Após aceitação da PROPOSTA, o **PREGOEIRO** verificará a HABILITAÇÃO do LICITANTE e, em seguida, anunciará o LICITANTE vencedor, que será convocado pelo **TRIBUNAL**, após homologação do resultado do **PREGÃO**, para assinar contrato ou instrumento equivalente no prazo e condições definidos neste Edital.

10.2. Como condição prévia ao exame da documentação de habilitação, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

a) SICAF (prova de regularidade fiscal federal, estadual e municipal e trabalhista);

b) Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS, mantido pela Controladoria-Geral da União (www.portaltransparencia.gov.br/sancoes/ceis);

c) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça (www.cnj.jus.br/improbidade_adm/consultar_requerido.php);

d) Lista de Inidôneos, mantida pelo Tribunal de Contas da União – TCU; (http://portal.tcu.gov.br/responsabilizacao-publica/licitantes-inidoneas/);

e) Consulta ao CNAE no sítio da Receita Federal https://www.receita.fazenda.gov.br/pessoajuridica/cnpj/cnpjreva/cnpjreva_solicitacao.asp.

10.2.1 As consultas referentes às alíneas "b", "c" e "d" podem ser substituídas pela Consulta Consolidada de Pessoa Jurídica, mantida pelo Tribunal de Contas da União – TCU (https://certidoes-apf.apps.tcu.gov.br/)

10.3. A consulta aos cadastros do item 10.2 será realizada em nome da empresa licitante e também do sócio (a) majoritário (a), por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio(a) majoritário(a).

10.4. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

10.5. O Pregoeiro, então, consultará o Sistema de Cadastro Unificado de Fornecedores – SICAF, em relação à habilitação da empresa licitante.

10.6. Poderão ser consultados os sítios oficiais emissores de certidões, especialmente quando o licitante esteja com alguma documentação vencida junto ao SICAF.

10.7. O licitante será convocado a encaminhar, via SISTEMA:

a) Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

a.1) Caso a licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices, deverá apresentar patrimônio líquido igual ou superior a 10% (dez por cento) do valor estimado para a contratação.

b) Certidão Negativa de Falência, recuperação judicial ou extrajudicial, expedida pelo Cartório Distribuidor da sede da Licitante, com emissão de até 60 dias da abertura da licitação;

b.1) No caso de certidão positiva de recuperação judicial ou extrajudicial, o licitante deverá apresentar a comprovação de que o respectivo plano de recuperação foi acolhido judicialmente, na forma do art. 58, da Lei n.º 11.101, de 09 de fevereiro de 2005, sob pena de inabilitação, devendo, ainda, comprovar todos os demais requisitos de habilitação.

c) Atestado(s) de capacidade técnico-operacional, fornecido(s) por pessoa(s) jurídica(s) de direito público e privado, devidamente identificada(s), em nome do licitante, relativo(s) a fornecimento de materiais e execução de atividades pertinentes e compatíveis em características, quantidades e prazos com os objetos da presente licitação.

10.8. Caso o Pregoeiro não logre êxito em obter as certidões correspondentes através do sítio oficial, na hipótese de se encontrarem vencidas no referido sistema ou no caso de documentos exigidos para a HABILITAÇÃO que não estejam contemplados no SICAF, deverão ser enviados pelo SISTEMA, no prazo máximo de **04 (quatro) horas,** após o encerramento da fase de lances ou da solicitação do **PREGOEIRO** no **SISTEMA**, conforme o caso, ressalvado o disposto quanto à comprovação da regularidade fiscal e/ou trabalhista das licitantes qualificadas como microempresas ou empresas de pequeno porte, conforme estatui o art. 43, § 1º da LC nº 123, de 2006.

10.9. O **PREGOEIRO**, constatando que a documentação apresentada pelo LICITANTE atende às exigências editalícias, proclamará HABILITADO o LICITANTE e, aquele que deixar de apresentar a documentação exigida ou apresentar de forma irregular será proclamado INABILITADO.

10.10. Sob pena de inabilitação, os documentos encaminhados para HABILITAÇÃO deverão estar em nome do LICITANTE, e preferencialmente, com o número do CNPJ e o respectivo endereço.

10.11. Se o LICITANTE for matriz, todos os documentos deverão estar em nome da matriz, e se o LICITANTE for filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

10.12. A existência de restrição relativamente à regularidade fiscal e trabalhista não impede que a licitante qualificada como microempresa ou empresa de pequeno porte seja declarada vencedora, uma vez que atenda a todas as demais exigências do edital.

10.12.1. A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.

10.13. Constatada a existência de alguma restrição no que tange à regularidade fiscal e/ou trabalhista de microempresas e empresas de pequeno porte, o certame será suspenso e a empresa será convocada para, no prazo de 5 (cinco) dias úteis, após a declaração do vencedor, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa, apresentada dentro dos primeiros 5 (cinco) dias úteis.

10.14. A não-regularização fiscal e/ou trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, com a reabertura da sessão pública.

10.15. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no *"chat"* a nova data e horário para a continuidade da mesma.

10.16. Será inabilitado o licitante que não comprovar sua habilitação, deixar de apresentar quaisquer dos documentos exigidos para a habilitação, ou apresentá-los em desacordo com o estabelecido neste Edital.

10.17. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

10.18. Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

10.19. A abertura da fase recursal em relação ao resultado do certame ocorrerá após os prazos de regularização fiscal e trabalhista de que trata o subitem 10.13.

10.20. Para fins de HABILITAÇÃO, a verificação em sítios oficiais de órgãos e entidades emissores de Certidões constitui meio legal de prova.

11. DOS RECURSOS ADMINISTRATIVOS

11.1. Declarado o vencedor, o **PREGOEIRO** abrirá prazo de 30 (trinta) a 40 (quarenta) minutos, em campo próprio do **SISTEMA**, para manifestação de intenção de recurso dos LICITANTES.

11.2. O LICITANTE que tiver sua intenção de Recurso aceita deverá registrar as razões do Recurso, em campo próprio do **SISTEMA**, no prazo de 3 (três) dias, ficando os demais LICITANTES, desde logo, intimados a apresentar contrarrazões, também via **SISTEMA**, em igual prazo, que começará a contar do término do prazo do LICITANTE Recorrente, sendo-lhes assegurada vista imediata dos autos. Decorridos esses prazos, o **PREGOEIRO** terá o prazo de 5 (cinco) dias úteis para proferir sua decisão. O acolhimento do Recurso importará na invalidação apenas dos atos insuscetíveis de aproveitamento.

11.3. Caso não reconsidere sua decisão, o **PREGOEIRO** submeterá o Recurso, devidamente informado, à consideração da Autoridade Superior do **TRIBUNAL**, que proferirá decisão definitiva. Decidido o Recurso, a autoridade competente fará a adjudicação do objeto da Licitação ao LICITANTE vencedor.

11.4. A falta de manifestação imediata e motivada da intenção de interpor Recurso, no momento da Sessão Pública, implica decadência desse direito, ficando o **PREGOEIRO** autorizada a adjudicar o serviço ao LICITANTE vencedor.

11.5. Os autos do Processo licitatório permanecerão com vista franqueada aos interessados na **COMISSÃO PERMANENTE DE LICITAÇÃO**, no endereço indicado neste Edital.

12. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

12.1. Declarado o vencedor e não havendo manifestação de Recursos, o **PREGOEIRO**, através do **SISTEMA** fará a adjudicação do objeto desta Licitação ao vencedor e, em seguida, a autoridade superior do **TRIBUNAL** homologará a Licitação.

12.1.1. Para os itens em que houver recurso, caberá à autoridade superior os procedimentos de adjudicação do objeto.

13. DA IMPUGNAÇÃO AO EDITAL

13.1. Até 2 (dois) dias úteis antes da data fixada para a abertura da Sessão Pública deste **PREGÃO**, qualquer pessoa poderá impugnar o Edital, na forma eletrônica.

13.2. Caberá ao **PREGOEIRO** decidir sobre a impugnação formulada, podendo, se for o caso, auxiliar-se pelo setor responsável pela elaboração do Termo de Referência e ainda pela Assessoria Jurídica do **TRIBUNAL**.

13.3. Se a impugnação contra o Edital for acolhida, o Edital será alterado e será definida e publicada nova data para realização do certame, pelo mesmo instrumento de publicação em que se deu o texto original. Caso a alteração no ato convocatório possa inquestionavelmente afetar a elaboração da PROPOSTA DE PREÇOS, o prazo inicialmente estabelecido será reaberto.

12.4. Decairá do direito de impugnar perante o **TRIBUNAL** os termos deste Edital aquele que, aceitando-os sem objeção, venha a apontar, depois do julgamento, falhas ou irregularidades que o viciariam, hipótese em que tal comunicação não terá efeito de recurso.

14. DO CONTRATO

14.1. Após a homologação, a contratação será formalizada pelo **TRIBUNAL** por meio de instrumento contratual nos moldes do Modelo da Minuta de Contrato - ANEXO II deste Edital, ou ainda, quando for o caso, pela emissão da nota de empenho, ordem de serviço ou outro instrumento similar, conforme dispõe o art. 62, da Lei nº 8.666/1993.

14.2. O Contrato a ser firmado terá suas cláusulas e condições reguladas pelas Leis nº 10.520/2002 e nº 8.666/1993 e pelo Decreto nº 5.450/2005, nos termos da Minuta do Contrato, ANEXO II deste Edital.

14.3. Após a assinatura do Contrato o **TRIBUNAL**, através da Coordenadoria de Licitações, Aquisições e Contratos, providenciará, até o quinto dia do mês subseqüente ao mês da assinatura do Contrato, a resenha do Contrato para publicá-la no Diário Oficial da União, até o vigésimo dia desse mês. A publicação do extrato resumido do Contrato poderá ser acompanhada pelo CONTRATADO no site www.in.gov.br.

15. DAS SANÇÕES ADMINISTRATIVAS

15.1. De acordo com a **CLÁUSULA NONA** da Minuta do Contrato – Anexo III deste Edital.

16. DA RESCISÃO

16.1. O **TRIBUNAL** poderá rescindir o Contrato desde que ocorra qualquer das hipóteses previstas no artigo 78, da Lei nº 8.666/93, com as conseqüências indicadas no seu artigo 80, sem prejuízo das sanções previstas naquela Lei e neste edital, nas condições estabelecidas na Minuta do Contrato, **ANEXO II** deste edital.

17. DO PAGAMENTO:

17.1. De acordo com a **CLÁUSULA TERCEIRA** da Minuta do Contrato – Anexo II deste Edital.

18. DAS OBRIGAÇÕES DO TRIBUNAL

18.1. A CONTRATANTE obriga-se a cumprir todas as exigências editalícias, inclusive as que estão estabelecidas na **CLÁUSULA QUARTA** da Minuta do Contrato – Anexo II deste Edital.

19. DAS OBRIGAÇÕES DA LICITANTE VENCEDORA

19.1. A CONTRATADA obriga-se a cumprir todas as exigências editalícias, inclusive as que estão estabelecidas na **CLÁUSULA QUINTA** da Minuta do Contrato – Anexo II deste Edital.

20. DAS DISPOSIÇÕES GERAIS

20.1. O edital deste **PREGÃO** se encontra disponível nos endereços eletrônicos www.comprasgovernamentais.gov.br e www.tre-ma.jus.br, assim como copiado mediante a apresentação de pendrive, para sua regravação.

20.2. Os pedidos de esclarecimentos referentes a esse procedimento licitatório deverão ser enviados ao **PREGOEIRO** até 03 (três) dias úteis antes da data fixada para abertura da Sessão Pública, exclusivamente por meio eletrônico, via internet, para o endereço: licitacao@tre-ma.jus.br.

20.3. É facultado ao **PREGOEIRO**, auxiliado pela equipe de apoio, proceder em qualquer fase desta licitação a diligências destinadas a esclarecer ou a complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar originalmente da **PROPOSTA.**

20.4. Caso não seja possível decidir de imediato sobre a aceitabilidade da **PROPOSTA** ou dos documentos de **HABILITAÇÃO,** o **PREGOEIRO** poderá suspender o **PREGÃO** e marcar nova data para sua aceitabilidade ficando intimados, no mesmo ato, os licitantes.

20.5. A apresentação da **PROPOSTA** de preços obriga o LICITANTE declarado vencedor ao cumprimento de todas as condições deste edital, sujeitando-se o licitante às sanções previstas neste edital e na legislação aplicada á espécie.

20.6. Quaisquer informações relativas a esta licitação serão prestados pelo **PREGOEIRO** e membros da equipe de apoio na **Seção de Análise e Licitação - SELIC,** localizada no primeiro andar do Anexo ao prédio sede do Tribunal Regional Eleitoral do Maranhão, situado na Av. Senador Vitorino Freire, s/n, Areinha, São Luís, através dos fones/fax: (98) 2107-8876/8802, ou pelo e-mail licitacao@tre-ma.jus.br, em dias úteis, de segunda a sexta-feira, no horário das 13 às 19h, obedecidos os seguintes critérios:

22.6.1. Em hipótese alguma serão aceitos entendimentos verbais entre interessados e o **TRIBUNAL**;

22.6.2. Os esclarecimentos aos consulentes serão comunicados a todos os demais interessados que tenham adquirido o presente Edital.

22.6.3. Os casos omissos serão resolvidos pelo **PREGOEIRO,** que decidirá com base nas normas conduzidas pela legislação em vigor aplicada à espécie.

20.7. Fazem parte integrante deste Edital o Anexo I – Termo de Referência e Anexo II - Minuta do Contrato.

São Luís, 05 de novembro de 2019.

KÁTIA LIMA SILVA MIRANDA

Chefe da SELIC

ANEXO I DO EDITAL
TERMO DE REFERÊNCIA

1. DETALHAMENTO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

1.1. DEFINIÇÃO DO OBJETO DA CONTRATAÇÃO

- Aquisição de solução de firewall composta de duas appliances em alta disponibilidade (HA) ativo/ativo, com garantia de 60 meses.

1.2. DESCRIÇÃO DOS BENS E/OU SERVIÇOS

Item	Bens
1	Solução de firewall tipo 1 – Next Generation Firewall (equipamento principal + equipamento de alta garantia) com instalação assistida, configuração e com garantia de 60 meses.
2	Solução de firewall tipo 2 - de pequeno porte com instalação assistida, configuração e com garantia de 60 meses.

1.3. ESPECIFICAÇÕES TÉCNICAS (REQUISITOS DA SOLUÇÃO)

Item	Bens
1	Solução de firewall tipo 1 – Next Generation Firewall (equipamento principal + equipamento de alta garantia), conforme as especificações do Subanexo I do termo de referência.
2	Solução de firewall tipo 2 - de pequeno porte, conforme as especificações do Subanexo I do termo de referência.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1.MOTIVAÇÃO

Motivação:

- A solução atualmente instalada no TRE-MA foi adquirida em 2013 composta por: Firewall SonicWall NSA 4500, 5500 na sede do Tribunal e TZs 200/SOHO para os locais remotos como: zonas eleitorais e postos de atendimento itinerante. Esta solução está em operação a mais de 6 anos e também com seu ciclo de vida e suporte no final, conforme documento publicado no site do fabricante no endereço: https://www.sonicwall.com/pt-br/support/product-lifecycle-tables/.

Diante deste cenário estamos propondo um pregão eletrônico para a aquisição de uma nova solução de firewall de próxima geração (Next Generation Firewall) juntamente com os firewalls de pequeno porte.

Foi estudada a possibilidade de atualização da solução atual pelo fabricante SonicWall, no entanto, ao enviar sua proposta, verificou-se que o custo apresentado está equiparado com outras propostas e licitações. Portanto, optamos por adquirir uma nova solução, ao invés de atualizar a solução atual. Tal escolha favorecerá a ampliação da competitividade, possibilitando que outras empresas participem, e permite também uma unificação de modelo e capacidade de processamento da solução.

Para o atendimento da demanda foram analisadas contratações de outros Regionais, como é o caso do Pregão Eletrônico n.º 61/2018 do Tribunal Regional Eleitoral da Bahia e do Pregão Eletrônico n.º 58/2018 do Tribunal Regional Eleitoral do Rio Grande do Sul, que tinham a mesma necessidade de substituição dos equipamentos que o TRE-MA possui.

Também foram consultados fornecedores que oferecem soluções de firewall para empresas/governo.

2.2. OBJETIVOS

Objetivo: *Adquirir uma solução de firewall que substitua a solução atual que está fora de garantia e desatualizada.*

2.3. RESULTADOS PRETENDIDOS

Resultado pretendido: *Garantir um ambiente seguro com dispositivos de segurança que implementem filtros que controlem as conexões e comunicações que trafegam de uma rede para outra, cujos filtros possuem a ação de permitir ou negar o acesso entre redes. Este dispositivo denominado de firewall tem várias características, as quais se destacam: ajudar a impedir que a rede, servidores e ativos sejam acessados sem autorização; evitar que informações sejam capturadas; bloquear programas indesejados na rede como compartilhamento de dados e de mensagens instantâneas; fechar portas não utilizadas, racionalizando o uso da Internet; permitir a auditoria nos acessos a recursos da rede; permitir a limitação da banda por serviços de monitoramento dos links de dados que passam pelo equipamento.*

2.4. ALINHAMENTO ESTRATÉGICO

Meta do PETIC: Índice de satisfação dos clientes – Garantir que as soluções de TIC satisfaçam os usuários e promovam a melhoria da percepção em relação aos atendimentos prestados pela área de TIC.

2.5. DEMANDA X QUANTIDADE (VOLUME DE BENS E/OU SERVIÇOS)

Item	Demanda Prevista	Previsão inicial (com memória de cálculo)
1	Solução de firewall (equipamento principal + equipamento de alta garantia) com instalação assistida, configuração e com garantia de 60 meses.	2 firewall x (R$ 453.650,23) = R$ 907.300,45
2	Solução de firewall de pequeno porte com instalação assistida, configuração e com garantia de 60 meses.	20 firewall x (R$ 5.815,23) = R$ 116.304,60

2.5 – PRODUTIVIDADE/CAPACIDADE MÍNIMA DE FORNECIMENTO DA SOLUÇÃO

Não se aplica

2.6. ANÁLISE DE MERCADO

O objeto da contratação é usual no mercado e a pesquisa mercadológica para a composição dos preços de referência observou os requisitos previstos na Instrução Normativa n. 5/2014 – SLTI/MP.

Para o atendimento da demanda foram analisadas contratações de outros Regionais, como é o caso do Pregão Eletrônico n.º 61/2018 do Tribunal Regional Eleitoral da Bahia e do Pregão Eletrônico n.º 58/2018 do Tribunal Regional Eleitoral do Rio Grande do Sul, que tinham a mesma necessidade de substituição dos equipamentos que o TRE-MA possui. Também foram consultados fornecedores que oferecem soluções de firewall para empresas/governo.

Optou-se, portanto, *pela aquisição, através de pregão eletrônico, de uma solução de firewall de próxima geração, juntamente com os firewalls de pequeno porte,* por ser esta a solução que melhor atende aos interesses da Administração, consoante justificativas apresentadas nos estudos preliminares.

2.7. NATUREZA DO OBJETO

Objeto de natureza comum, cujos padrões de desempenho e qualidade podem ser objetivamente definidos, por meio de especificações usuais de mercado. Configura uma solução de tecnologia da informação.

2.8. PARCELAMENTO DO OBJETO

Opta-se pelo não parcelamento do objeto dada a necessidade de perfeita integração/compatibilidade entre o Firewall de próxima geração e os firewalls de pequeno porte, principalmente nos itens que se referem a serviços. Ou seja, garantir que um serviço disponível no item 1 seja utilizado pelo item 2, como por exemplo (IPS, Antivírus e Anti-Spyware). Evitar escolher um fornecedor de firewall que emprega estruturas de design e gerenciamento de interfaces de usuário totalmente diferentes entre gerações de produtos, complicando a implantação e trazendo curvas de aprendizado acentuadas.
Assim, em face dos obstáculos para imputar responsabilidades individualizadas, procurou-se evitar tal situação, a fim de buscar o adequado funcionamento dos itens e também salvaguardar as respectivas garantias.

2.9. CRITÉRIOS PARA ADJUDICAÇÃO

Será considerada vencedora a empresa que apresentar, além dos requisitos exigidos no Termo de Referência e Edital, a proposta com o menor preço global. A adjudicação do objeto será, portanto, global.

2.10. FORMA E CRITÉRIOS PARA A SELEÇÃO DO FORNECEDOR

A contratação será realizada por meio de pregão eletrônico, sendo selecionada a proposta que atender às especificações técnicas e o critério do menor preço, não sendo aceitos valores maiores que os estimados neste instrumento.
A licitante apta ao exercício do direito de preferência estabelecido no Decreto n. º 7.174/2010 deverá declarar, em campo próprio do Sistema, que atende aos requisitos previstos na legislação.

2.11. IMPACTO AMBIENTAL

Não se aplica

2.12. CONFORMIDADE TÉCNICA/LEGAL

Não existem normas técnicas ou legais que impactem na solução.

3. OBRIGAÇÕES CONTRATUAIS

3.1. OBRIGAÇÕES DO CONTRATANTE

3.1.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;
3.1.2. Encaminhar formalmente a demanda, preferencialmente por meio de Ordem de Serviço ou Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;
3.1.3. Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas, com a emissão dos Termos de Recebimento Provisório e Definitivo;

3.1.4. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis.
3.1.5. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em Contrato;
3.1.6. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da Solução de Tecnologia da Informação;
3.1.7. Verificar a regularidade da situação fiscal da Contratada antes de efetuar o pagamento devido;
3.1.8. Promover o acompanhamento e a fiscalização durante a vigência da garantia, anotando em registro próprio as falhas detectadas e comunicando as ocorrências de quaisquer fatos que exijam medidas corretivas por parte da contratada.

3.2. OBRIGAÇÕES DA CONTRATADA

3.2.1. Entregar o objeto deste Termo de Referência ao TRE-MA dentro do prazo e especificações do edital;
3.2.2. Indicar formalmente preposto apto a representá-la junto ao TRE-MA, que deverá responder pela fiel execução do contrato;
3.2.3. Atender prontamente quaisquer orientações e exigências do fiscal do contrato, inerentes à execução do objeto contratual;
3.2.4. Reparar quaisquer danos diretamente causados ao TRE-MA ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, sendo que a fiscalização ou o acompanhamento da execução dos serviços pelo TRE-MA não exclui ou reduz a responsabilidade;
3.2.5. Comunicar por escrito, quando verificar condições inadequadas para a prestação da garantia técnica e atualização de versões, apresentando razões justificadoras, que serão objeto de apreciação pelo TRE-MA;
3.2.6. Propiciar todos os meios e facilidades necessárias à fiscalização da Solução de Tecnologia da Informação pelo TRE-MA, cujo representante terá poderes para sustar o fornecimento, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária;
3.2.7. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;
3.2.8. Manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para prestar a garantia correspondente à Solução de Tecnologia da Informação;
3.2.9. Manter a produtividade ou a capacidade mínima de fornecimento da Solução de Tecnologia da Informação durante a execução do contrato;
3.2.10. Disponibilizar acesso a serviço telefônico 0800 ou similar e acesso web para abertura e acompanhamento de chamados, sugestões e esclarecimento de dúvidas, durante todo o período da garantia dos equipamentos e softwares.
3.2.11. Aceitar os acréscimos e supressões de até 25% (vinte e cinco por cento) propostos pela Administração, conforme previsto no art. 65, § 1º, da Lei 8.666/93.
3.2.12. Fornecer equipamentos novos e realizar os serviços de instalação com a qualidade adequada.
3.2.13. A Contratada deverá apresentar, se for o caso, comprovação da origem dos bens importados oferecidos e da quitação dos tributos de importação a eles referentes, que deve ser apresentada no momento da entrega do objeto, sob pena de rescisão contratual e multa.

4. MODELO DE EXECUÇÃO DA CONTRATAÇÃO

4.1. ROTINAS DE EXECUÇÃO

4.1.1. O local de entrega dos equipamentos e de prestação dos serviços é o Datacenter localizado no prédio anexo do Tribunal Regional Eleitoral do Maranhão, localizado na Av. Senador Vitorino Freire, Areinha, São Luís-MA, CEP: 65.010-917, em dias úteis das 13h às 18h.

4.1.2. O prazo de entrega e instalação dos equipamentos será de 60 dias corridos, contados do recebimento da ordem de fornecimento.

4.1.2.1 Caso a contratada não confirme o recebimento em até 24 horas, o prazo de entrega e instalação será contado a partir do segundo dia subsequente a data do envio da ordem de fornecimento.

4.1.2.2 A instalação e configuração poderá ser rejeitada, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência, devendo ser corrigidos no prazo de 10 dias corridos, a contar da notificação da contratada às suas custas, sem prejuízo da aplicação de penalidades.

4.1.3. Caso se perceba a impossibilidade de cumprir o prazo estipulado para a disponibilização de bens, incluindo sua instalação e configuração, a vencedora do certame deverá apresentar, até a data de vencimento fixada, justificativas escritas e devidamente comprovadas, **afastando a possibilidade de aplicação de penalidade**, apoiando o pedido de prorrogação em um ou mais dos seguintes fatos:

4.1.3.1. Ocorrência de fato superveniente, excepcional ou imprevisível, estranho à vontade das partes, que altere fundamentalmente as condições do contrato;

4.1.3.2. Impedimento decorrente de fato ou ato de terceiros, reconhecido pela Administração em documento contemporâneo à sua ocorrência;

4.1.4. O objeto poderá ser rejeitado, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituído ou refeito em até 30 dias corridos, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

4.1.5. O objeto de contratação, incluindo os serviços de instalação e migração, somente será aceito de forme provisória quando todas as funcionalidades estiverem com status operacionais.

4.1.6. O recebimento definitivo, inclusive dos serviços de instalação e migração, se dará no prazo de 10 (dez) dias após o recebimento provisório e após a verificação da conformidade com as especificações constantes deste instrumento e desde que constatada a estabilidade operacional da solução implantada.

4.2. FORMAS/MEIOS DE COMUNICAÇÃO

As formas de comunicação entre contratante e contratada poderão se dar por email, ofício ou sistema informatizado.

4.3. FORMA DE PAGAMENTO

4.3.1. O pagamento será efetuado, por meio de ordem bancária, em até 30(trinta) dias contados do **recebimento definitivo do objeto**, formalizado por meio de atesto da nota fiscal pelo Fiscal do Contrato.

4.3.2. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

4.3.3. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será

providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da Contratante.

4.3.4. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

4.3.5. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, sem prejuízo da aplicação de penalidade.

4.3.6. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

4.4. MODELOS DE ANEXOS

Subanexo I – Especificações técnicas dos equipamentos.

5. MODELO DE GESTÃO DA CONTRATAÇÃO

5.1. FORMA DE SOLICITAÇÃO

A solicitação para o fornecimento de bens e serviços será feita por meio de ordem de fornecimento emitida pelo gestor do contrato.

5.2. – RECURSOS HUMANOS PARA GESTÃO E FISCALIZAÇÃO

Gestor do Contrato

Convocar e realizar reunião inicial entre CONTRATANTE e CONTRATADA quando necessário.
Analisar desvios de qualidade e aderência.
Solicitar correções à CONTRATADA, baseadas na informação sobre desvios de qualidade ou aderência apontados pelos fiscais.
Indicar sanções para aplicabilidade pela Área Administrativa.
Autorizar a emissão da nota fiscal à CONTRATADA, quando necessário.
Solicitar saneamento das irregularidades à CONTRATADA.

Fiscal Administrativo

Verificar regularidades fiscais, trabalhistas e previdenciárias.
Encaminhar as irregularidades ao Gestor do Contrato, para verificar se são sanáveis.

Fiscais Demandante, Técnico

Avaliar qualidade e aderência aos termos contratuais
Atestar os serviços prestados pela Contratada
Atestar a Nota Fiscal elaborada pela Contratada

5.3. VALORES/PROCEDIMENTOS PARA RETENÇÃO OU GLOSA

Não se aplica, considerando que não foram previstos Acordos de Níveis de Serviço.

5.4. INFRAÇÕES CONTRATUAIS/SANÇÕES ADMINISTRATIVAS

5.4.1. Cometerá infração administrativa aquele que:

5.4.1.1. Inexecução total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

5.4.1.2. Não entregar quaisquer documentos exigidos neste Termo de Referência, no Edital ou no Contrato;

5.4.1.3. Apresentar documentação falsa;

5.4.1.4. Ensejar retardamento da execução do objeto;

5.4.1.5. Falhar ou Fraudar na execução do serviço;

5.4.1.6. Comportar-se de modo inidôneo;

5.4.1.7. Cometer fraude fiscal;

5.4.1.8. Não mantiver a proposta;

5.4.1.9. Não assinar o contrato ou a ata de registro de preços.

5.4.2. Consideram-se comportamentos inidôneos, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP e o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

5.4.3. Pelo cometimento de infrações administrativas, a Licitante/Contratada ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

5.4.3.1. Advertência por faltas leves, assim entendidas aquelas que não acarretarem prejuízos significativos à Administração;

5.4.3.2. Multa moratória de 0,5% (cinco décimos por cento) sobre o valor da Ordem de Fornecimento por dia de atraso injustificado no cumprimento dos prazos de entrega e instalação, até o limite de 20 (vinte) dias corridos, após o que restará configurada a inexecução total do objeto, passível de rescisão contratual – a critério da Administração – e aplicação de multa específica;

5.4.3.3. Multa moratória de 0,5% (cinco décimos por cento) sobre o valor do equipamento por dia de atraso injustificado na assistência técnica (resolução de problemas) prevista nas condições de garantia, até o limite de 20 (vinte) dias corridos, após o que restará configurada a inexecução parcial, sujeitando a Contratada à multa compensatória de até 10% (dez por cento) do valor total do contrato;

5.4.3.4. Multa compensatória de até 10% (trinta por cento) sobre o valor da Ordem de Fornecimento, no caso de inexecução total do objeto e nas hipóteses previstas nos subitens 5.4.1.2 a 5.4.1.9., proporcional ao prejuízo ocasionado pelo inadimplemento da obrigação;

5.4.3.5. Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida, como por exemplo, entregar o equipamento e não configurá-lo, não realizar o treinamento.

5.4.3.6. Impedimento de licitar e contratar coma União pelo prazo de até 05 (cinco) anos, nas hipóteses previstas nos subitens 5.4.1.2 a 5.4.1.9.

5.4.4. Caso a Contratada não comprove a origem dos bens importados e/ou a quitação dos tributos de importação a eles referentes, será aplicada multa de 5% (cinco por cento) sobre o valor de contratação.

5.4.5. As penalidades serão obrigatoriamente registradas no SICAF e, no caso de impedimento de licitar, a CONTRATADA deverá ser descredenciada por igual período, sem prejuízo das demais cominações legais.

5.4.6. A penalidade de multa poderá ser aplicada cumulativamente com outras sanções e será descontada dos pagamentos devidos pelo TRE-MA ou, caso seja necessário, cobrada judicialmente.

5.5.– EMISSÃO DE NOTA FISCAL/PAGAMENTO

Item	Bens / Serviços	Custo Unit.	Qte	Custo Total	Fonte (Programa / Ação)
1	Solução de firewall (equipamento principal + equipamento de alta garantia) com instalação assistida, configuração e com garantia de 60 meses	R$ 453.650,23	2	R$ 907.300,45	449040 – EQUIPAMENTOS DE INFORMÁTICA
2	Solução de firewall de pequeno porte) com instalação assistida, configuração e com garantia de 60 meses	R$ 5.815,23	20	R$ 116.304,60	
Total:				**R$ 1.023.605,05**	

6. REGIME DE EXECUÇÃO DA CONTRATAÇÃO

Não se aplica

7. QULAIFICAÇÃO TÉCNICA

A LICITANTE deverá apresentar atestado de capacidade técnico-operacional fornecido por pessoa jurídica de direito público ou privado devidamente identificada, em nome do licitante, relativo a fornecimento de materiais e execução de atividades pertinentes e

compatíveis em características, quantidades e prazos com os objetos da presente licitação.

8. CRITÉRIOS TÉCNICOS DE JULGAMENTO
Menor preço

9. IDENTIFICAÇÃO DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO	
Fiscal Demandante e substituto:	Lourencio Monteiro de Melo e Sebastião da Silva Penha
Fiscal Técnico e substituto:	Lourencio Monteiro de Melo e Sebastião da Silva Penha
Fiscal Administrativo e substituto:	Jaime Monteiro da Silva Júnior e Roseana Maria Fernandes Santos de Sousa
Gestor e substituto:	Jaime Monteiro da Silva Júnior e Roseana Maria Fernandes Santos de Sousa

10 – DECLARAÇÃO DA EQUIPE DE PLANEJAMENTO		
Declaro que este Termo de Referência foi elaborado com base nos Estudos Preliminares constantes do processo administrativo digital (PAD) nº 4296/2019.		
Integrante Técnico	**Integrante Demandante**	**Integrante Administrativo**
_____ Lourencio Monteiro de Melo	_____ Lourencio Monteiro de Melo	_____ Marco Aurélio Martins

SUBANEXO I
ESPECIFICAÇÕES TÉCNICAS

1.1. Detalhamento dos bens e serviços que compõem a solução

1.1.1. Fornecimento de serviços de suporte técnico para a solução de eventuais problemas que possam ocorrer nos equipamentos de firewall pelo período da garantia, incluindo substituições de hardwares quando necessário, durante a vigência da garantia dos equipamentos;

1.1.2. Todas as funcionalidades descritas nos requisitos técnicos deverão funcionar no mesmo appliance sem a necessidade de composição de um ou mais produtos;

1.1.3. O equipamento deverá ser baseado em hardware desenvolvido como dispositivo de segurança tipo firewall, ou seja, não sendo aceitas soluções baseadas em plataforma PC ou equivalente.

1.1.4. Fornecimento e ativação das licenças dos serviços nos firewalls, pelo período de garantia dos equipamentos;

1.1.5. Fornecimento dos serviços de instalação dos novos equipamentos, configuração, migração de todos os objetos e regras do firewall, configuração de VPNs entre firewall concentrador e firewalls de pequeno porte, configuração como roteador entre as Vlans dos usuários e a Vlan dos servidores, configuração de pelo menos 5 regras de firewall para pelo menos 5 servidores de rede, enfim, todos os serviços para a efetiva migração da solução de firewall do Tribunal até alcançar plena estabilidade operacional;

1.1.6. Os novos equipamentos deverão manter a mesma arquitetura existente no TRE-MA em cluster de firewall funcionando com duas appliances em alta disponibilidade (HA), podendo ser ativo-ativo ou ativo-passivo, sendo os gateways de segurança idênticos em cluster, garantindo que em caso de falha de um equipamento o outro assuma o processamento evitando a indisponibilidade dos serviços oferecidos pelo datacenter;

1.1.7. Treinamento para a equipe de técnicos do Tribunal composta de 5 (cinco) pessoas, podendo o treinamento ser na modalidade "in company";

1.1.8. Os equipamentos deverão ser novos, estarem em linha de produção, terem o fim do ciclo de vida superior a 5 (cinco) anos a partir da entrega, ou seja, não serão aceitos equipamentos em modo "End of Life e End of Support";

1.1.9. **Deve ter garantia total de pelo menos 5 (cinco) anos, com garantia de funcionamento**. Esta exigência visa garantir a funcionalidade e disponibilidade da solução que se pretende adquirir, a qual é de extrema criticidade dentro do datacenter do TRE-MA, uma vez que o Firewall tem por objetivo aplicar e manter uma política de segurança na rede de computadores deste Tribunal. A garantia contratada nestes termos, além de ser uma prática recorrente no mercado, afasta a temeridade de haver interrupção na prestação de assistência técnica e uma possível indisponibilidade dos serviços suportados pela solução de firewall do TRE-MA, evitando a ocorrência de incidentes da rede. Ademais, esse requisito de garantia tem um melhor custo/benefício para a Administração, considerando os custos elevados de uma possível contratação de extensão de garantia, conforme demonstrado pelo Doc. PAD n.º 92020/2019.

1.1.10. As atualizações de assinaturas dos serviços, tais como, AntiSpam, antivírus, etc. e atualizações de software e suporte técnico 24x7 deverão ocorrer por pelo menos 5 (cinco) anos;

1.1.11. Deverão ser fornecidos todos os cabos, suportes, parafusos e porca gaiola para a instalação dos equipamentos em rack 19´´;

Requisitos técnicos

1.2. Firewall tipo 1 - Next Generation Firewall.

1.2.1. Os equipamentos de firewall CONCENTRADOR deverão ter, **no mínimo**, as seguintes características técnicas:

1.2.1.1. Mínimo de 9 Gbps de statefull Throughput;
1.2.1.2. Mínimo de 6 Gbps de IPS Throughput;
1.2.1.3. Mínimo de 3 Gbps de Application Inspection Throughput;
1.2.1.4. Mínimo de 5.4 Gbps de Anti-Malware Throughput;
1.2.1.5. Mínimo de 1.6 Gbps de DPI Throughput;
1.2.1.6. Mínimo de 3 Gbps de VPN Throughput;
1.2.1.7. Mínimo de 02 Interfaces SFP+ de 10 GbE ativas/licenciadas. Os gbics para cada interface devem ser fornecidos junto com o equipamento;
1.2.1.8. Mínimo de 16 portas GbE, sendo que destas no mínimo 8 portas devem ser de 1 GbE (Ethernet RJ45). Caso as outras interfaces sejam fibra, os gbics para cada interface devem ser fornecidos junto com os equipamentos e se essas interfaces forem de velocidades diferentes de 1Gbps elas devem permitir que sejam configuradas para trabalhar na velocidade de 1Gbps;
1.2.1.9. Possuir no mínimo 01 interface de 1 GbE dedicada para gerenciamento e 01 para console;
1.2.1.10. Possuir no mínimo 1 (uma) interface dedicada para sincronismo de estados da solução de alta disponibilidade;
1.2.1.11. Deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, sem custos adicionais;
1.2.1.12. Suporte no mínimo 400 interfaces de Vlan (802.1q);
1.2.1.13. Deve ser fornecido com dupla ventilação;
1.2.1.14. Deve ser fornecido com fonte redundante;
1.2.1.15. Capacidade mínima de 2000 túneis VPNs IPSEC Site-to-site já licenciadas;
1.2.1.16. Capacidade mínima de 2000 túneis VPNs IPSEC Client-to-Site já licenciadas;
1.2.1.17. Ter capacidade de no mínimo 1000 túneis SSL VPN, devendo fornecer os equipamentos com no mínimo 100 conexões já licenciadas por pelo menos 5 (cinco) anos;
1.2.1.18. Implementar protocolo DHCP Relay;
1.2.1.19. O equipamento deve ser fornecido com a capacidade máxima de memória e processamento;
1.2.1.20. Deve possibilitar a visualização da utilização dos recursos de CPU, memória, armazenamento interno e atividade de rede na sua interface de gerência e/ou em sistema de gerência centralizado;
1.2.1.21. Deve implementar decriptografia e inspeção de tráfego SSL. Esta funcionalidade já deve estar licenciada por pelo menos 5 (cinco) anos;
1.2.1.22. Deve implementar administração/controle de largura de banda (QoS);
1.2.1.23. Deve suportar os protocolos:
(a) IPV4 e IPV6;
(b) VLAN 802.1.q
(c) Agregação de links 802.3x;
(d) DHCP e DHCPv6;
(e) NTP;
(f) Roteamento estático e dinâmico em IPv4 e dinâmico IPv6;
(g) Roteamento RIP v1/v1, OSPF v2 ou OSPF v3 ou BGP v4;
(h) Deve suportar SNMP v2c ou SNMP v3;

1.2.1.24. Deve permitir acesso ao equipamento via CLI (console), SSH e interface web HTTPS;

1.2.1.25. Deve possuir funcionalidade de backup/restore da configuração e políticas de segurança;

1.2.1.26. Ter capacidade de suporte de até 60 mil novas conexões/segundo;

1.2.1.27. Deve possuir a funcionalidade de acelerador WAN;

1.2.1.28. Deve possuir a capacidade de identificação de ataques como: ataques direcionados, Zero Day, exploração de vulnerabilidades, indicadores de ofuscação e indicadores de comprometimentos automáticos, mesmo que necessite de licenciamento específico para esta finalidade;

1.2.1.29. Deverá ser fornecido com pelo menos 2 (duas) fontes de alimentação independentes, redundantes e hot-swappable, com alimentação nominal 100~120AC e 210~230AC e frequência 50 ou 60 Hz.

1.2.2. Devem ser fornecidas todas as licenças de software com no mínimo as seguintes características:

1.2.2.1. A Contratada deverá fornecer licenças com validade de 60 (sessenta) meses, tal exigência é comum no mercado pois é disponível em sites de fabricantes de equipamentos o período exigido como tempo de garantia, nos serviços dos itens "a" ao "f" que compõem a solução de firewall:

a) Antivírus e antispyware;
b) Serviço de prevenção contra intrusão;
c) Controle de aplicações (aplication control);
d) Serviço de filtragem de conteúdo;
e) Serviço de suporte técnico na modalidade de 24x7 (24 horas/dia e 7 dias/semana);
f) Atualizações e upgrades de softwares e firmwares.

1.2.2.2. O licenciamento deve prover a atualização automática e em tempo real dos filtros de conteúdo WEB, através da categorização contínua de novos sites da internet, dos mecanismos de prevenção a intrusão e recursos de segurança contra novos vírus, spywares, vulnerabilidades de softwares e códigos maliciosos;

1.2.3. As atualizações e upgrades de software e firmware devem ser disponibilizadas à CONTRATANTE para download no site da CONTRATADA ou do fabricante;

1.2.4. O serviço de suporte técnico pelo período contratado deverá ser prestado através do acionamento da CONTRATADA, para atendimento das necessidades de informação e restabelecimento de funcionalidades nas condições e prazos a seguir:

1.2.4.1. SEVERIDADE BAIXA – prazo máximo de 48 horas para solução: correção de falha que não impede a continuidade da maior parte dos negócios e solicitações de informações sobre os produtos, incluindo configuração e instalação;

1.2.4.2. SEVERIDADE MÉDIA – prazo máximo de 24 horas para solução: problemas que causem impactos significativos nos negócios incluindo degradação de desempenho;

1.2.4.3. SEVERIDADE ALTA – prazo máximo de 06 horas para solução: os serviços se encontrarem indisponíveis;

1.2.5. Ocorrendo problemas técnicos ou físicos nos equipamentos cuja recuperação ao status operacional fique prejudicada, durante a vigência da garantia, a contratada deverá substituir os equipamentos envolvidos;

1.2.6. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
1.2.7. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
1.2.8. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
1.2.9. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
1.2.10. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
1.2.11. O gerenciamento da solução deve suportar a interface de administração via web no próprio dispositivo de proteção de rede;
1.2.12. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;
1.2.13. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 8023ad e LACP;
1.2.14. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
1.2.15. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
1.2.16. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
1.2.17. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
1.2.18. Os dispositivos de proteção de rede devem suportar sFlow ou NetFlow;
1.2.19. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
1.2.20. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
1.2.21. Deve suportar NAT dinâmico (Many-to-1);
1.2.22. Deve suportar NAT dinâmico (Many-to-Many);
1.2.23. Deve suportar NAT estático (1-to-1);
1.2.24. Deve suportar NAT estático (Many-to-Many);
1.2.25. Deve suportar NAT estático bidirecional 1-to-1;
1.2.26. Deve suportar Tradução de porta (PAT);
1.2.27. Deve suportar NAT de Origem;
1.2.28. Deve suportar NAT de Destino;
1.2.29. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
1.2.30. Deve suportar NAT64 ou NAT46;
1.2.31. Deve implementar balanceamento de link com persistência de sessão;
1.2.32. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;
1.2.33. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
1.2.34. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
1.2.35. Enviar log para sistemas de monitoração externos, simultaneamente;

1.2.36. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
1.2.37. Proteção anti-spoofing;
1.2.38. Implementar otimização do tráfego entre dois equipamentos;
1.2.39. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
1.2.40. Para IPv6, deve suportar roteamento estático ou dinâmico (OSPFv3);
1.2.41. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
1.2.42. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
1.2.43. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
1.2.44. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha visibilidade do tráfego;
1.2.45. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;
1.2.46. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;
1.2.47. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 2 equipamentos no cluster;
1.2.48. A configuração em alta disponibilidade deve sincronizar: Sessões;
1.2.49. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;
1.2.50. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
1.2.51. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;
1.2.52. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;
1.2.53. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
1.2.54. Em alta disponibilidade, deve ser possível o uso de clusters, seja ativo-ativo ou ativo-passivo;
1.2.55. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS);
1.2.56. Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados;

1.2.57. Controle por Política de Firewall
  1.2.57.1. Deverá suportar controles por zona de segurança;
  1.2.57.2. Controles de políticas por porta e protocolo;
  1.2.57.3. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
  1.2.57.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança
  1.2.57.5. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS);
  1.2.57.6. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);

1.2.57.7. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
1.2.57.8. Deve descriptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;
1.2.57.9. Controle de inspeção e descriptografia por política;
1.2.57.10. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
1.2.57.11. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);
1.2.57.12. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações;
1.2.57.13. Suporte a objetos e regras IPV6;
1.2.57.14. Suporte a objetos e regras multicast;
1.2.57.15. Deve suportar no mínimo três tipos de resposta nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Reject, Accept;
1.2.57.16. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.2.58. Controle de Aplicações
1.2.58.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
1.2.58.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
1.2.58.3. Reconhecer pelo menos 2200 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
1.2.58.4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
1.2.58.5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
1.2.58.6. Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Bittorrent e aplicações VOIP que utilizam criptografia proprietária;
1.2.58.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
1.2.58.8. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
1.2.58.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo

também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex;

1.2.58.10. Identificar o uso de táticas evasivas via comunicações criptografadas;
1.2.58.11. Atualizar a base de assinaturas de aplicações automaticamente;
1.2.58.12. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
1.2.58.13. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
1.2.58.14. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
1.2.58.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
1.2.58.16. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
1.2.58.17. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
1.2.58.18. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL;
1.2.58.19. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
1.2.58.20. Deve alertar o usuário quando uma aplicação for bloqueada;
1.2.58.21. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
1.2.58.22. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
1.2.58.23. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
1.2.58.24. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
1.2.58.25. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como:
   a) Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
   b) Nível de risco da aplicação;
   c) Categoria da aplicação.

1.2.59. Prevenção de Ameaças
1.2.59.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

1.2.59.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
1.2.59.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante, garantindo que o equipamento fique operacional mesmo fora de garantia;
1.2.59.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
1.2.59.5. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante e enviar tcp-reset;
1.2.59.6. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
1.2.59.7. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
1.2.59.8. Possibilidade de definir regras de IPS para hosts específicos, ou criar exceções por IP de origem ou de destino em regras ou assinaturas;
1.2.59.9. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
1.2.59.10. Deve permitir o bloqueio de vulnerabilidades;
1.2.59.11. Deve permitir o bloqueio de exploits conhecidos;
1.2.59.12. Deve incluir proteção contra-ataques de negação de serviços;
1.2.59.13. Deverá possuir o seguinte mecanismos de inspeção de IPS:
1. Análise de padrões de estado de conexões;
2. Análise de decodificação de protocolo;
3. Análise para detecção de anomalias de protocolo;
4. Análise heurística;
5. IP Defragmentation;
6. Remontagem de pacotes de TCP;
7. Bloqueio de pacotes malformados.

1.2.59.14. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
1.2.59.15. Detectar e bloquear a origem de portscans;
1.2.59.16. Bloquear ataques efetuados por worms conhecidos;
1.2.59.17. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
1.2.59.18. Possuir assinaturas para bloqueio de ataques de buffer overflow;
1.2.59.19. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
1.2.59.20. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
1.2.59.21. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMTP e POP3;
1.2.59.22. Suportar bloqueio de arquivos por tipo;
1.2.59.23. Identificar e bloquear comunicação com botnets;
1.2.59.24. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação,

usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

1.2.59.25. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

1.2.59.26. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

1.2.59.27. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

1.2.59.28. Os eventos devem identificar o país de onde partiu a ameaça;

1.2.59.29. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

1.2.59.30. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

1.2.59.31. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc., ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;

1.2.60. Filtro de URL

1.2.60.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.2.60.2. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

1.2.60.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

1.2.60.4. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;

1.2.60.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

1.2.60.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

1.2.60.7. Possuir pelo menos 60 categorias de URLs;

1.2.60.8. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

1.2.60.9. Permitir a customização de página de bloqueio;

1.2.60.10. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir ao usuário continuar acessando o site);

1.2.61. Identificação de Usuários

1.2.61.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração

com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

1.2.61.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;

1.2.61.3. Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2;

1.2.61.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso;

1.2.61.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;

1.2.61.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;

1.2.61.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

1.2.61.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

1.2.61.9. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

1.2.61.10. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso à internet e gerenciamento da solução;

1.2.61.11. Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator;

1.2.62. QoS e Traffic Shaping

1.2.62.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

1.2.62.2. Suportar a criação de políticas de QoS e Traffic Shaping por:

1. Endereço de origem;
2. Endereço de destino;
3. Usuário e grupo;
4. Aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
5. Porta;

1.2.62.3. O QoS deve possibilitar a definição de tráfego:

1. Com banda garantida;

2. Com banda máxima;
3. De fila de prioridade;

1.2.62.4. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP e aplicações como Skype;
1.2.62.5. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
1.2.62.6. Suportar modificação de valores DSCP para o Diffserv;
1.2.62.7. Suportar priorização de tráfego usando informação de Type of Service;
1.2.62.8. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
1.2.62.9. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;

1.2.63. Filtro de Dados
1.2.63.1. Permitir a criação de filtros para arquivos e dados pré-definidos;
1.2.63.2. Os arquivos devem ser identificados por extensão e tipo;
1.2.63.3. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
1.2.63.4. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
1.2.63.5. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
1.2.63.6. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

1.2.64. Geo Localização
1.2.64.1. Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados;
1.2.64.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
1.2.64.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;

1.2.65. VPN
1.2.65.1. Suportar VPN Site-to-Site e Cliente-To-Site;
1.2.65.2. Suportar IPSec VPN;
1.2.65.3. Suportar SSL VPN;
1.2.65.4. A VPN IPSEc deve suportar:
1. 3DES;
2. Autenticação MD5 e SHA-1;
3. Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
4. Algoritmo Internet Key Exchange (IKEv1 e v2);
5. AES 128, 192 e 256 (Advanced Encryption Standard);
6. Autenticação via certificado IKE PKI

1.2.65.5. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
1.2.65.6. Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
1.2.65.7. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

1.2.65.8. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
1.2.65.9. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
1.2.65.10. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
1.2.65.11. Atribuição de DNS nos clientes remotos de VPN;
1.2.65.12. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
1.2.65.13. Suportar autenticação via AD/LDAP e base de usuários local;
1.2.65.14. Suportar leitura e verificação de CRL (certificate revocation list);
1.2.65.15. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
1.2.65.16. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma:
1. Antes do usuário autenticar na estação;
2. Após autenticação do usuário na estação;
3. Sob demanda do usuário.

1.2.65.17. Deverá manter uma conexão segura com o portal durante a sessão;
1.2.65.18. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

1.3. Firewall tipo 2 – De pequeno porte.

1.3.1. Estes equipamentos deverão contemplar os serviços de suporte no mínimo na modalidade 8x5 (oito horas/dia e 5 dias/semana) para o período de 60 (sessenta) meses. O equipamento ofertado deve possuir, no mínimo, as características técnicas do modelo de referência SonicWall SOHO Wireless que é utilizado pelo TRE-MA e atende atualmente os requisitos técnicos de estabelecimento de VPN (rede privada virtual) na solução instalada no TRE-MA, dentre os requisitos temos em destaque as seguintes características:
1.3.1.1. Deve possuir no mínimo 4 interfaces 10/100/1000 Gbe. Todas operando em modo autosense e em modo half/full duplex, com inversão automática de polaridade configuráveis pelo administrador do firewall para atender os segmentos de segurança e rede para:
1. Segmento WAN, ou externo;
2. Segmento LAN ou rede interna;
3. Segmento LAN ou rede interna podendo ser configurado com DMZ (zona desmilitarizada);
4. Segmento LAN ou rede interna ou porta de sincronismo para funcionamento em alta disponibilidade;
5. Segmento ou Zona dedicada para controle de dispositivos wireless dedicado com controle e configuração destes dispositivos;

1.3.1.2. A fonte de alimentação deve ser com operação automática entre 110/220V;
1.3.1.3. Possuir performance de firewall throughput igual ou superior a 300 Mbps;
1.3.1.4. Deve possuir proteção Anti-Malware integrado no mesmo appliance;

1.3.1.5. Possuir a capacidade mínima de conexões suportadas em modo firewall de 10.000 (dez mil) conexões;
1.3.1.6. Deve suportar no mínimo 1.800 novas conexões por segundo;
1.3.1.7. O equipamento deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, onde o mesmo deverá ser descriptografado de forma transparente a aplicação;
1.3.1.8. Possuir performance de VPN IPSEC (3DES & AES 256) de 75 Mbps ou superior;
1.3.1.9. Deve ter a capacidade de prover servidor DHCP interno suportando múltiplos escopos de endereçamento para a mesma interface e a funcionalidade de DHCP Relay;
1.3.1.10. Deve suportar no mínimo 10 túneis VPN IPSEC do tipo site-to-site já licenciados;
1.3.1.11. Deve suportar no mínimo 5 túneis VPN IPSEC do tipo client-to-site, devendo disponibilizar junto com cada equipamento no mínimo 01 licença/conexão, sem custo adicional;
1.3.1.12. Deve suportar no mínimo 10 conexões clientes tipo SSL, devendo disponibilizar junto com cada equipamento no mínimo 01 licença/conexão, sem custo adicional;
1.3.1.13. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;
1.3.1.14. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, certificados digitais e XAUTH client authentication;
1.3.1.15. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda de circuito primário;
1.3.1.16. Deve permitir utilização de LDAP, AD e RADIUS;
1.3.1.17. Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e LDAP;
1.3.1.18. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente através de regras de firewall DPI (Deep Packet Inspection) sem a necessidade de uma nova autenticação como, por exemplo, para os serviços de navegação a internet atuando assim de forma toda transparente ao usuário. Serviços como HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2008/2012 com AD;
1.3.1.19. Deve ter a capacidade de suportar no mínimo 250 usuários autenticados com serviços ativos e identificados, passando por este tipo de segurança. Políticas baseadas por grupos de usuários deverão ser suportadas por este dispositivo;
1.3.1.20. Deve permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas de administração;
1.3.1.21. Deve possibilitar gerência remota, com interface gráfica nativa;
1.3.1.22. Permitir a visualização de estatísticas do uso de CPU, memória da máquina onde o firewall está rodando e tráfego de rede em todas as interfaces do firewall através da interface gráfica remota, em tempo real;

1.3.1.23. Os produtos de hardware ofertados devem ser novos, nunca terem sido utilizados e não terem sido descontinuados, ou seja, devem constar na linha atual de comercialização;

1.3.1.24. O equipamento deverá ser baseado em hardware para firewall, não em plataforma X86 ou equivalente;

1.3.2. A CONTRATADA deverá auxiliar a CONTRATANTE em todo o processo de renovação de todas as licenças e atualização de todos os hardwares contratados, dentre eles: gerar e fornecer os arquivos necessários, executar a renovação no portal de gerência do fabricante para todos os firewalls, e demais demandas que forem necessárias;

1.4.Serviço De Instalação/Migração e Treinamento Hands-on

1.4.1. A licitante deverá fornecer ao Tribunal os seguintes serviços:

1.4.1.1. Treinamento para a equipe de técnicos do Tribunal composta de 5 (cinco) pessoas, podendo o treinamento ser na modalidade "in company", com carga horária mínima de 24h;

1.4.1.2. Os serviços de instalação dos novos equipamentos, configuração, migração de todos os objetos e regras de firewall, configuração de VPNs entre firewall concentrador e firewalls de pequeno porte, configuração dos firewalls como roteador entre as Vlans dos usuários e dos servidores, criação de pelo menos 5 regras de firewall para pelo menos 5 servidores de aplicação, enfim, todos os serviços para a efetiva migração da solução de firewall do Tribunal até alcançar plena estabilidade operacional;

1.4.2. Tais serviços devem ser realizados obedecendo aos seguintes critérios:

1.4.2.1. **SERVIÇO DE INSTALAÇÃO/MIGRAÇÃO**

a) A licitante vencedora deverá disponibilizar técnicos devidamente certificados junto ao fabricante da solução ofertada para realizar todos os serviços de instalação/migração;
b) Os técnicos designados para os serviços de instalação/migração deverão possuir experiências no processo de implantação de solução de firewall, demonstrada via atestado de capacidade técnica, que deverão ser apresentados no momento de efetiva prestação dos serviços;
c) Toda configuração existente em termos de enlace de redes, VPNs, rotas, objetos e regras de firewalls, etc., deverão ser migrados para a nova solução ofertada;
d) Deverá ser criada pelo menos 5 regras de firewall para pelo menos 5 servidores de aplicações do TRE-MA;
e) Configuração de VPNs entre a solução de firewall com equipamento Contivity existente no TRE-MA;
f) Todos os serviços serão assistidos pela equipe da Seção de Suporte a Redes Locais do Tribunal, a qual dará todo o apoio e condições necessárias para a realização das atividades;
g) O serviço de instalação e migração somente serão aceitos de forma provisória quando todas as funcionalidades estiverem com status operacionais;
h) O recebimento definitivo dos serviços de instalação e migração se dará no prazo de 10 (dez) dias após o recebimento provisório e se for constatada a estabilidade operacional da solução implantada;

1.4.2.2. **TREINAMENTO HANDS-ON**

a) O curso deverá abranger todos os recursos técnicos da solução ofertada em nível avançado de configuração e gerenciado da solução;
b) Deverá disponibilizar material didático oficial para cada treinamento;
c) Cada treinando que atingir as exigências do treinamento deverá receber Certificado;
d) O treinamento poderá ser realizado na modalidade "in company", com carga horária mínima de 24 (vinte e quatro) horas;
e) Para a realização do curso deverá ser utilizado equipamentos iguais aos ofertados para fins de realização das baterias de exercícios e laboratórios;

1.5. Solução de Gerenciamento Centralizado

1.5.1. Deve permitir gerenciar ao menos 30 dispositivos;
1.5.2. Deve ser fornecido em virtual appliance;
1.5.3. Deverá ser compatível com ambiente VMware ESXi 5.5 e 6.0, Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2 e Citrix XenServer 6.0+;
1.5.4. Não deve possuir limite na quantidade de múltiplas vCPU caso entregue como appliance virtual;
1.5.5. Não deve possuir limite para suporte a expansão de memória RAM caso entregue como appliance virtual;
1.5.6. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
1.5.7. Permitir acesso concorrente de administradores;
1.5.8. Possuir interface baseada em linha de comando para administração da solução de gerência
1.5.9. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
1.5.10. Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;
1.5.11. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
1.5.12. Gerar alertas automáticos via:
  1.5.12.1. Email;
  1.5.12.2. SNMP;
  1.5.12.3. Syslog.
1.5.13. Deve suportar backup/restore de todas as configurações da solução de gerência, permitindo ao administrador agendar backups da configuração em um determinado dia e hora;
1.5.14. Deve ser permitido ao administrador transferir os backups para um servidor:
  1.5.14.1. FTP;
  1.5.14.2. SCP;
  1.5.14.3. SFTP.
1.5.15. As alterações realizadas em um servidor de gerência deverão ser automaticamente replicadas para o servidor redundante;
1.5.16. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através:
  1.5.16.1. De contas de usuários LOCAIS;
  1.5.16.2. De base externa TACACS;
  1.5.16.3. De usuários de base externa LDAP;
  1.5.16.4. De base externa RADIUS;
  1.5.16.5. De Certificado Digital X.509 (PKI).

1.5.17. Deve suportar sincronização do relógio interno via protocolo NTP;
1.5.18. Deve registrar as ações efetuadas por quaisquer usuários;
1.5.19. Devem ser fornecidos manuais de instalação, configuração e operação de toda a solução, na língua portuguesa ou inglesa, com apresentação de boa qualidade;
1.5.20. Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência;
1.5.21. Deve permitir habilitar e desabilitar, para cada interface de rede da solução de gerência, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet;
1.5.22. Deve permitir virtualizar a solução de gerência, de forma que cada administrador possa gerenciar, visualizar e editar apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado;
1.5.23. A solução de gerência deve permitir criar administradores que tenham acesso à todas as instâncias de virtualização;
1.5.24. Deve suportar XML API;
1.5.25. Deve suportar JSON API;
1.5.26. O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;
1.5.27. O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
1.5.28. O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;
1.5.29. Permitir localizar quais regras um objeto está sendo utilizado;
1.5.30. Deve atribuir sequencialmente um número a cada regra de firewall;
1.5.31. Deve atribuir sequencialmente um número a cada regra de DOS;
1.5.32. Deve possuir capacidade de criação e gerenciamento de regras SD-WAN;
1.5.33. Permitir criação de regras que fiquem ativas em horário definido;
1.5.34. Permitir backup das configurações e rollback de configuração para a última configuração salva;
1.5.35. Deve possuir mecanismo de Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
1.5.36. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
1.5.37. Deve permitir que todos os controladores/concentradores sejam controlados de forma centralizada utilizando apenas um servidor de gerência;
1.5.38. A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta.
1.5.39. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances;
1.5.40. Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;
1.5.41. Deve permitir criar fluxos de aprovação na solução de gerência, onde um administrador possa criar todas as regras, mas as mesmas somente sejam aplicadas após aprovação de outro administrador;
1.5.42. Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos;
1.5.43. Permitir que eventuais políticas e objetos já presentes nos dispositivos sejam importados quando o mesmo for adicionado à solução de gerência;
1.5.44. Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como hostname, serial, IP de gerência, licenças, horário do sistema e firmware;

1.5.45. Possuir "wizard" na solução de gerência para instalação de políticas e configurações dos dispositivos;
1.5.46. Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;
1.5.47. Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos;
1.5.48. Possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência
1.5.49. Permitir configurar e visualizar balanceamento de links nos dispositivos gerenciados de forma centralizada;
1.5.50. Permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos;
1.5.51. Deve permitir criar regras de NAT64 e NAT46 de forma centralizada;
1.5.52. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;
1.5.53. Permitir criar, a partir da solução de gerência, VPNs entre os dispositivos gerenciados de forma centralizada, incluindo topologia (hub, spoke, dial-up), autenticações, chaves e métodos de criptografia;

1.6. Garantia e suporte

1.6.1. Deverá possuir garantia mínima de 60 (sessenta) meses para os equipamentos, incluindo a atualização de software (correções, "patches", "updates" ou novas "releases") no regime 24x7, 24 (vinte e quatro) horas por dia e 7(sete) dias por semana, incluindo feriados e finais de semana;
1.6.2. Deverá possuir Tempo de solução, conforme a severidade especificada no subitem 1.2.4, a partir da abertura do chamado técnico para falhas de hardware ou software
1.6.3. Deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos;
1.6.4. Deverá possuir um sistema atendimento de suporte.

ANEXO II DO EDITAL

(MINUTA DO CONTRATO)

TERMO DE CONTRATO QUE ENTRE SI CELEBRAM A UNIÃO, ATRAVÉS DO TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO, E A EMPRESA....., CONFORME PREGÃO ELETRÔNICO Nº 52/2019 (PROCESSO PAD N.º 10.973/2019), TENDO POR OBJETO A **AQUISIÇÃO DE SOLUÇÃO DE FIREWALL COMPOSTA DE DUAS APPLIANCES EM ALTA DISPONIBILIDADE (HA) ATIVO/ATIVO.**

A **UNIÃO,** por intermédio do **TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO,** nesta ato denominado **CONTRATANTE,** inscrito no CNPJ Nº 05.962.421/0001-17, com sede na Av. Senador Vitorino Freire, s/n, em São Luís-MA, neste ato representado por seu Presidente, **DES.** _____, portador do R.G. nº _____-SSP/____ e do CPF nº. _____, e, de outro lado, a empresa _____, inscrita no CNPJ-MF, sob o nº_____, estabelecida **(inserir endereço completo),** neste ato denominada **CONTRATADA,** representada por **(inserir o cargo),** senhor(a) **(qualificação do signatário do contrato),** portador da Cédula de Identidade nº _____e CPF(MF) nº_____de acordo com a representação legal que lhe é outorgada por ____**(inserir qual dos instrumentos: procuração/contrato social/estatuto social)** resolvem celebrar o presente Contrato para **aquisição de solução de firewall composta de duas appliances em alta disponibilidade (HA) ativo/ativo,** em conformidade com a **Lei nº 10.520/002, Lei n.º 8.666/93, Lei Complementar nº 123/2006 e Decreto Federal nº 5.450/2005**, mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – OBJETO

1.1. O presente Contrato tem por objeto a **aquisição de solução de firewall composta de duas appliances em alta disponibilidade (HA) ativo/ativo,** obedecidas as condições do instrumento convocatório e respectivos anexos.

CLÁUSULA SEGUNDA – DO PREÇO

2.1. O presente contrato tem o valor total de **R$ .....** (por extenso).

CLÁUSULA TERCEIRA - DO PAGAMENTO

3.1. O Pagamento correspondente será efetuado à Contratada por meio de ordem bancária, no prazo máximo de 30 dias, após o recebimento definitivo do objeto e atesto da respectiva nota fiscal/fatura.

3.2 O processo de pagamento será iniciado com a fatura/nota fiscal apresentada pela Contratada, com atesto do Fiscal do Contrato de que os serviços foram prestados corretamente, bem como os documentos de comprovação da regularidade fiscal junto as Fazendas Federal, Estadual e Municipal, Seguridade Social – INSS, FGTS e Certidão Negativa de Débitos Trabalhistas;

3.3 Caso seja detectado qualquer problema na documentação acima, será concedido prazo para regularização. Findo este, em permanecendo a inércia da Contratada, a mesma será apenada com multa prevista em capítulo próprio, podendo ser cumulada com rescisão contratual.

3.4. Caso se verifique erro na fatura, esta não será atestada até sua retificação pela CONTRATADA.

3.5. Qualquer atraso ocorrido na apresentação dos documentos por parte da CONTRATADA importará em prorrogação automática do prazo de vencimento da obrigação do CONTRATANTE.

3.6. Nos casos de eventuais atrasos de pagamento, desde que a licitante vencedora não tenha concorrido de alguma forma para tanto, fica convencionado que os encargos moratórios devidos pelo TRE, entre a data acima referida e a correspondente ao efetivo pagamento da nota fiscal/fatura, será calculado por meio da aplicação da seguinte fórmula:

EM = I x N x VP, onde:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela em atraso.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = \frac{i}{365} \qquad I = \frac{6/100}{365} \qquad I = 0{,}00016438$$

Onde i = taxa percentual anual no valor de 6%.

3.7. Não será efetuado qualquer pagamento à CONTRATADA enquanto houver pendência de liquidação da obrigação financeira em virtude de penalidade ou inadimplência contratual;

3.8. Deverão ser observadas as demais disposições do item 4.3 do Anexo I – Termo de Referência.

CLÁUSULA QUARTA: DAS OBRIGAÇÕES DO CONTRATANTE

4.1. O CONTRATANTE obriga-se a cumprir as condições estabelecidas no ITEM 3.1 do Termo de Referência - ANEXO I deste Edital.

CLÁUSULA QUINTA - OBRIGAÇÕES DA CONTRATADA

5.1. A CONTRATADA obriga-se a cumprir todas as exigências do edital, inclusive as estabelecidas no ITEM 3.2 do Termo de Referência - ANEXO I deste Edital.

5.2. A CONTRATADA obriga-se a comprovar, em se tratando de bens ou serviços de informática ou automação, a origem dos bens importados oferecidos e a quitação dos tributos de importação a eles referentes, que deve ser apresentada no momento da entrega do objeto, sob pena de rescisão contratual e multa de 10% (dez por cento) sobre o valor do contrato/empenho.

CLÁUSULA SEXTA – VIGÊNCIA

6.1. A vigência do contrato será de **06 (seis) meses**, a contar do primeiro dia útil após a data de sua publicação e observará o disposto no art. 57 da Lei 8.666/1993, **ressalvados os prazos de garantia**.

CLÁUSULA SÉTIMA - ALTERAÇÃO

7.1. Este instrumento poderá ser alterado na ocorrência de quaisquer dos fatos constantes no artigo 65 da Lei n º 8.666/93.

CLÁUSULA OITAVA - DOTAÇÃO ORÇAMENTÁRIA

8.1. As despesas com a execução do presente Contrato correrão à conta do Orçamento Geral da União, aprovado para o exercício financeiro de 2019, cuja classificação funcional programática e categoria econômica é a seguinte:

.....

PARÁGRAFO ÚNICO – DO EMPENHO

Para cobertura das despesas relativas ao presente Contrato, foi emitida a Nota de Empenho nº. 2019NExxxxxx, à conta da dotação especificada neste contrato.

CLÁUSULA NONA - PENALIDADES

9.1. São aplicáveis as sanções previstas no ITEM 5.4 do Termo de Referência – Anexo I do edital.

9.2. São aplicáveis ainda as penalidades da Lei 10.520/2002.

PARÁGRAFO ÚNICO - DESCONTO DO VALOR DA MULTA

Se o valor das multas não for pago ou depositado na Conta Única do Tesouro Nacional, será automaticamente descontado de qualquer fatura ou crédito a que a **CONTRATADA** vier a fazer *jus*.

CLÁUSULA DÉCIMA – RECURSOS

10.1. Caberá recurso nos casos previstos na Lei de Licitações, devendo o mesmo ser protocolado e dirigido ao Presidente do TRE/MA, por intermédio da autoridade que praticou o ato recorrido.

CLÁUSULA DÉCIMA PRIMEIRA – RESCISÃO

11.1. O presente Contrato poderá ser rescindido de acordo com o que estabelecem os artigos 77 a 80, da Lei nº 8.666/93, mediante notificação através de ofício entregue diretamente ou por via postal, com prova de recebimento, sem prejuízo do disposto na cláusula nona.

CLÁUSULA DÉCIMA SEGUNDA– DISPOSIÇÕES GERAIS

12.1. Aplica-se a este Contrato o disposto no artigo 58, da Lei nº 8.666/93.

12.2. As partes contratantes ratificam todas as condições preestabelecidas no instrumento convocatório e na proposta da licitante, independentemente de transcrição.

CLÁUSULA DÉCIMA TERCEIRA - FORO

13.1. Fica eleito o Foro da Seção Judiciária da Justiça Federal da Capital do Estado do Maranhão, para dirimir as questões derivadas deste Contrato.

E por estarem de acordo, depois de lido e achado conforme, foi o presente Contrato lavrado em quatro cópias de igual teor e forma, assinado pelas partes e testemunhas abaixo.

São Luís - MA, ... de ..... de 2019.

TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO
Presidente

CONTRATADA
Representante

TESTEMUNHAS:

1. NOME: .....
CIC: .....

2.NOME: .....
CIC: .....